Hireserve ATS
How we protect your data

As the GDPR approaches, it's important that you understand what measures are in place to keep your data secure in Hireserve ATS.

Ahead of the GDPR, some of you have asked for further detail about our approach to information security and our supporting policies. As such, we've collated your key questions in this document and provided answers below to support your supplier due-diligence and for you to share with colleagues in your IT, Compliance and Procurement teams.

What approach does Hireserve take to information security?

Hireserve is ISO 27001 accredited, demonstrating that robust, sustainable and lawful data protection and information security processes are firmly embedded in the company's day-to-day working practices. Hireserve's Head of Technology oversees information security in close collaboration with the Information Security Manager.

Does Hireserve have a Data Protection Officer?

Under the GDPR, Hireserve is not required to appoint a Data Protection Officer due to the size of the business; however, the company recognises the importance of this position and as such has appointed Hireserve's Head of People as the Information Security Manager. Ultimately, responsibility for data protection and information security lies with the Board, as detailed in Hireserve's Data Protection Policy.

What policies does Hireserve have to support its commitment to information security and data protection?

The company has a full Information Security Management System (ISMS), which incorporates a number of policies including (but not limited to):

- Data Protection policy
- Access Control policy
- Network System Monitoring policy
- Password policy
- Virus Protection policy
- Security Incident Reporting policy

Where is Hireserve's data stored?

For UK, EU, Asia and international customer organisations, data is stored in dual data centres run by Rackspace in the UK. For public sector and education customers in Canada, data is held on the Microsoft Azure platform in dual data centres in Quebec and Toronto.

What is Hireserve's procedure for reporting data leaks and/or security violations?

Hireserve has a robust incident reporting process, which is supported by the company's Security Incident Reporting policy.

Does Hireserve ATS undergo regular penetration testing?

All customers are able to request a penetration test of the system whenever they wish. Hireserve has facilitated a number of these tests for customers in the past. The company plans to introduce a bi-annual penetration test and is in the process of selecting a suitable supplier.

What access control and information security measures does Hireserve take?

- ✓ All passwords for Hireserve ATS back office and candidate portals are hashed and encrypted
- ✓ Back office and candidate portals can only be accessed via https
- ✓ Secure cookies are used
- ✓ All Hireserve staff members accessing the database do so from workstations with encrypted drives and via a secure VPN connection
- ✓ Third party integrations run over https
- ✓ TLS support is offered for outgoing emails
- ✓ IDS (Intruder Detection Scanning) is in place
- ✓ All team members have undertaken information security training
- ✓ Data protection best practice is in place for physically stored data, with securely locked files and rooms and clear policies around storing and deleting/archiving data.

What back-up processes does Hireserve have in place?

Two weeks of backups are retained using a weekly schedule. A full back-up is taken on the first day of the week, with incremental back-ups taking place daily and ongoing archive logs backup taking place at regular intervals throughout each day. This process ensures that the database can be recovered to any point in time during the previous week. Old back-up copies that are not in the two-week retention period will be deleted.

GDPR functionality within Hireserve ATS

Hireserve is delivering a range of new features and tools within Hireserve ATS to help you, our customers, meet your data controller responsibilities under the GDPR.

- ✓ Configurable data retention period
- ✓ Automatic removal of candidates (via deletion or anonymisation) once they have passed your data retention threshold
- ✓ Mechanism to obtain consent or share a link to your privacy statement when candidates apply
- ✓ Updated 'Candidate Details' screen with new 'Data Protection' tab
- ✓ ...and more

Find out more: Download your GDPR Functionality guide on the Hub to learn more about new GDPR tools and features.

Check for personal data on other platforms and cookies...

Do remember to check other platforms your organisation is using where personal data might be being captured. For example, we are aware that some organisations' Google Analytics platforms have captured candidate email addresses as part of a candidate portal URL. If you are unintentionally capturing personal data in this manner, you will need to delete it permanently. In the first instance, ask your IT team if they can help you to identify if you are capturing personal data on different platforms. In addition, please be mindful that Hireserve places cookies on your careers site, about which you may need to inform candidates in your privacy statement. If you would like to learn more about which cookies are used by Hireserve ATS on your careers site, please refer to the FAQs on the Hireserve Hub.